



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/622,047

08/23/2000

Alexandr Andreevich Moldovyan

P65855US0

4150

136

7590

09/14/2006

JACOBSON HOLMAN PLLC
400 SEVENTH STREET N.W.
SUITE 600
WASHINGTON, DC 20004

EXAMINER

LANIER, BENJAMIN E

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 09/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/622,047

Applicant(s)

MOLDOVYAN ET AL.

Examiner

Benjamin E Lanier

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 August 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3 and 5 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3 and 5 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 23 August 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.


KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 22 August 2006 have been fully considered but they are not persuasive. Applicant appears to be repeating the argument that Schneier does not disclose permuting subkey bits depending on data subblock, which is not persuasive because Schneier specifically discloses that during each round of the DES algorithm, the key bits are shifted and then 48 bits are selected from the 56 bits of the key (page 270). This operation of permuting this subkey is described by Schneier as one of the key four operations that comprise the Function f performed during each round of the algorithm. This Function f includes multiple permutation operations (page 270).
2. Applicant argues that "The Examiner has incorrectly interpreted the conversion operation f appeared on page 270 and in Fig. 12.1 as an operation of permuting bits of subkey K_1 . In fact, the conversion operation f is not a permutation operation." This argument is not persuasive because Schneier discloses that:
 3. "In each round (see Figure 12.2), the key bits are shifted, and then 48 bits are selected from the 56 bits of the key." (From Page 270)
 4. Schneier goes on to discuss that the shifting of the key bits is done by either one or two bits, depending on the round (page 272). Each subkey is run through this compression permutation (page 273). Therefore, Schneier shows that the subkeys for each round of the DES operation are in fact shifted using a permutation function.

Art Unit: 2132

5. Applicant is incorrectly analyzing the actual Function f when discussing permutation of the subkeys (Remarks pages 2-3). Schneier shows that the keys are shifted prior to be applied in the Function f (pages 270, 272-273).
6. Applicant's argument that "Thus, in algorithm DES, the bit permutation operation is performed on the key by depending on the number of the round, but not on the data subblock, i.e. the feature of performing the subkey bit permutation operation depending on the data subblock being converted." This argument is not persuasive because each round has a specific **data subblock** associated with it. Figure 12.1 shows that in round 1, subkey K1 and data subblock R0 are operated on by Function f to produce an output that is then XOR'd with data subblock L0. In round 2, subkey K2 and data subblock R1 are operated on by Function f to produce an output that is then XOR'd with data subblock L1, and so on. Therefore, the DES algorithm described by Schneier clearly shows that each round of the algorithm utilizes specific data subblocks. So any bit permutation on the subkeys that is performed depending on the number of the round, is also dependent on a specific data subblock, because it is that specific subblock that will be operated on along with the subkey in question during that specific round. Applicant appears to be importing meaning into the claims that simply is not present in the claim language.
7. Applicant's argument with respect to claim 5 does not address Schneier, but is merely a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1, 3 rejected under 35 U.S.C. 102(b) as being anticipated by Schneier. Referring to claim 1, Schneier discloses the DES algorithm wherein a 64-bit block of plain text is split into a right half and a left half (Page 270), which meets the limitation of breaking down a data block into $N \geq 2$ subblocks. The encryption key is broken up into 16 subkeys (Figure 12.1), which meets the limitation of generating an encryption key in the form of a set of subkeys. There are 16 rounds of identical operations in which the data are combined with the key (Page 270 & Figure 12.1). The operations performed are exclusive or (Xor) operations (Page 270 & Figure 12.1), which meets the limitation of alternatively converting said data subblocks by performing a two-place operation on the data subblock and the subkey because figure 12.1 shows the exclusive or operation being performed on the subblock and the subkey. An exclusive or (Xor) operation is a two-place operation. In each round the key bits are shifted depending on a subblock (Page 270 & Figure 12.1), which meets the limitation of prior to carrying out said two-place operation on an I-th data subblock and a subkey, an operation of permuting subkey bits is performed on the subkey depending on the value of the j-th data subblock where i is not equal to j, because figure 12.1 shows that the data subblock L_0 is exclusive or'd with the result of the permutation function on subkey K_i that depends on data subblock R_0 . Therefore, from figure 12.1 (looking at one round for an example), L_0 would meet the limitation of the i-th data subblock, R_0 would meet the limitation of the j-th data subblock, K_1 would meet the limitation of the subkey being permuted, and function f would meet the limitation of the permutation function.

Art Unit: 2132

Referring to claim 3, Schneier discloses that each round the subkey bits are shifted depending on a subblock as discussed above (Page 270 & Figure 12.1), which meets the limitation of an operation of an operation of cyclic offsetting subkey bits depending on the j-th subblock is used as the j-th subblock-dependent operation of permuting subkey bits because the permutation function on the subkeys are performed each round and that would be considered cyclical.

Referring to claim 5, Schneier discloses that the subkeys are shifted as a result of a permutation function that depends on the j-th data subblock as discussed above (Page 270 & Figure 12.1). In the later rounds of the algorithm (see figure 12.1, specifically the calculation for R2), the permutation function operates on subkey K2 dependant upon the result of R1 data block calculation. The R1 data block calculation involved subkey K1, and therefore, the calculation of R2 also includes data from subkey K1, which meets the limitation of the operation of permuting subkey bits is performed on one of said set of subkeys depending on the value of the j-th data subblock, where i is not equal to j, and the value of another subkey.

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

Art Unit: 2132

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.


11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Benjamin E. Lanier



KAMBIZ ZAND
PRIMARY EXAMINER